Srihari Humbarwadi

227, Guruprasad Colony,
Belagaum KA IN 590006
Portfolio: http://www.sriharihumbarwadi.com

(+91) 7019552068
sriharihumbarwadi97@gmail.com

SKILLS

- Strong analytical and problem solving ability.
- Good understanding of web security practices, OWASP top 10.

EDUCATION

Belagavi, Karnataka **KLS Gogte Institute of Technology** **Aug. 2014 – Present**

- B.E. in Computer Science and Engineering. Percentage *(up to 7th semester)*: 65%
- 10th percentage (95.96%), 12th percentage (95%, PCM)

TECHNICAL EXPERIENCE AND PROJECTS

- **Detecting ransomware delivery using deep neural networks** *(python)*: The delivery of ransomware/malware can be detected by using *timing* and *URI* microbehaviors as features for DNN. This model classifies each network capture file (PCAP) as benign or exploit – if classified as exploit it alerts the sysadmin to take further actions. Eg: Apply new GPO for the AD. **(**originally researched by Rod Soto and Joseph Zadeh**)**
- **Text to speech** *(AWS POLLY, SQS, LAMBDA*): Simple web application using AWS services to convert given input into speech, with option to change the accent.
- **URL Shortener** *(Android, Java)*: Offers to shorten the input of long URL into a short and easily exchangeable URL, the short URL can be user defined.
- **Network reconnaissance** *(PowerShell, .NET)*: Scans the network for any intruders, and has option to scan open ports for a given node.
- **HID based key stroke injection** *(Arduino, embedded C, PowerShell):* Programmed a arduino based chip to behave as a HID device (keyboard) and send keystrokes when plugged in. Eg: Upon plugging in, it is capable of quickly running a one liner TCP reverse shell command on PowerShell, or steal saved passwords from Google Chrome.
- **Reverse Shell with backdoor-ed executable *(Fully undetected)*** *(PowerShell*): Created a reverse shell payload and backdoor-ed it inside an executable. The code was obfuscated to avoid triggering the anti-virus software.
- **Containerized Steam** *(Docker, Linux*): Created a docker image to run steam containerized, with support for GPU acceleration. The image was tested to run 10 parallel instances of steam on a single host OS successfully.

ADDITIONAL EXPERIENCE

- Generated vulnerability Assessment report for a well-known college, and helped to get the vulnerabilities patched.
- First Place, algorithmic coding event – “Knightron”.
- Solved 200+ coding problems on online platforms (Hackerearth, Hackerrank, Leetcode).
- Solved good number of CTFs on online platforms (Vulnhub).

Languages and Technologies

- **Languages**: C++, Python, bash.
- **Frameworks and Technologies**: Docker, AWS, HTML, CSS, burp suit, metasploit, Git versioning, Keras, scikit-learn, pytorch.